

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

JAN 27 1999

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)

Communications Assistance for)
Law Enforcement Act)

CC Docket No. 97-213

To: The Commission

**REPLY COMMENTS OF THE CELLULAR
TELECOMMUNICATIONS INDUSTRY ASSOCIATION
REGARDING FURTHER NOTICE OF PROPOSED
RULEMAKING**

Michael Altschul
Vice President and General Counsel
Randall S. Coleman
Vice President
Regulatory Policy & Law

**Cellular Telecommunications Industry
Association**
1250 Connecticut Ave., N.W.
Suite 800
Washington, D.C. 20036
(202) 785-0081

No. of Copies rec'd 0+10
List ASCDE

CONTENTS

SUMMARY	i
I. SECTION 107 GIVES THE COMMISSION AUTHORITY TO REJECT THE PUNCH LIST BASED ON THE COST OF CALEA, AND ITS IMPACT ON SUBSCRIBER RATES AND COMPETITION	4
A. The "Whether" and "How" of Section 107.....	6
B. Punch List Alternatives	10
C. DOJ's Incremental Cost Argument	11
D. Gold-Plating the Standard	14
E. Carrier Data.....	15
II. JSTD-025 AMENDMENT	17
A. DOJ's Unlawful Delegation Claim	17
B. DOJ's Proposal for a Rulemaking in Lieu of Ballot Resolution.....	18
C. DOJ's Call for Strict Compliance with the 180-day Amendment Cycle.....	20
D. Delay in Revising the Standard	22
E. The Role of the Enhanced Surveillance Standard ("ESS").....	23
F. The Need for Specificity in the Final Order.....	25
G. Compliance Date	26
III. REASONABLY AVAILABLE CALL-IDENTIFYING INFORMATION	27
IV. THE PUNCH LIST	31
A. The National Wiretap Plan	32
B. CALEA Is Not a Strict Liability Statute.....	34
C. Post-Cut-Through Digit Extraction	36
V. CONCLUSION	39

SUMMARY

The Cellular Telecommunications Industry Association ("CTIA") submits these Reply Comments in response to the Federal Communications Commission ("Commission") Further Notice of Proposed Rulemaking ("FNPRM"), dated November 5, 1998, and comments received by the Commission regarding the scope of the assistance capability requirements of the Communications Assistance for Law Enforcement Act ("CALEA").

The weight of comments argues against the FNPRM tentative conclusions insofar as they propose to add several of the punch list features to the industry standard. In particular, the Commission expressly should reject the new DOJ twist on CALEA that calls for a nation-wide wiretap plan for wireless carriers. And, the Commission should reject the notion that any network signal is reasonably available and must be provided to law enforcement, whatever the cost, whatever the technical difficulty.

Even if the Commission does hold that some of the punch list items are required, it can only promulgate a final rule that will yield the most cost-efficient implementation of CALEA with the least impact on subscriber rates, competition, and the introduction of new technologies. The Commission must reject DOJ's "CALEA AT ANY COST" approach because Section 107(b) does not allow the Commission to

trade off privacy, competition, innovation or impact on rates against enhanced surveillance features. The final rule must satisfy all of Section 107(b)'s factors.

Finally, DOJ no longer objects to remand to TR45.2 of any changes in the standard so long as the technical committee is held to a strict schedule and the Commission promulgates the final product. All commenters are in substantial agreement on the need for a remand. It is only the process and timing that are still in dispute. The Commission should permit the amendment of JSTD-025 through the normal industry process rather than the unworkable and extraordinary process proposed by DOJ.

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
)
Communications Assistance for) CC Docket No. 97-213
Law Enforcement Act)
)

To: The Commission

**REPLY COMMENTS OF THE CELLULAR
TELECOMMUNICATIONS INDUSTRY ASSOCIATION
REGARDING FURTHER NOTICE OF PROPOSED
RULEMAKING**

The Cellular Telecommunications Industry Association ("CTIA")¹ submits these Reply Comments in response to the Federal Communications Commission ("Commission") Further Notice of Proposed Rulemaking ("FNPRM"), dated November 5, 1998, and comments received by the Commission regarding the scope of

¹ CTIA is the principal trade association of the wireless telecommunications industry. Membership in the association encompasses all providers of commercial mobile radio services and includes 48 of the 50 largest cellular and personal communications services providers as well as others with an interest in the wireless communications industry.

the assistance capability requirements of the Communications Assistance for Law Enforcement Act ("CALEA").²

In its initial comments ("CTIA Comments"), CTIA disagreed with the FNPRM tentative conclusions insofar as they proposed to add several of the punch list features to the industry standard. Indeed, all those that commented, other than law enforcement, agreed that the punch list exceeds the scope of CALEA.

As CTIA pointed out, the FNPRM suffered from a lack of legal analysis to support any conclusion of law that certain punch list items were required by CALEA. In failing to give definition to the components of call-identifying information, and not defining when call-identifying information is reasonably available, the FNPRM reached incorrect legal conclusions, however tentative.

By fostering what Churchill once called "terminological inexactitude," the Commission may actually prolong the dispute. Ambiguity certainly does a disservice to all future efforts to comply with CALEA through a safe harbor standard. Without legal clarity, the Commission can be sure that it will see deficiency petitions again and again for every new technology as law enforcement seeks to expand the traditional notion and industry understanding of what is basically call setup information. In its final order, the Commission must reject DOJ's de facto definition of call-identifying

² *In the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Further Notice of Proposed Rulemaking* (adopted October 22, 1998, released

information (anything that may be useful to an investigation) in favor of the narrow terms Congress itself used to describe it (dialing or signaling used to route calls).

Further, even if the Commission seeks to adopt its now tentative conclusions, it can only promulgate a final rule based upon conclusions of law and findings of fact that the technical requirements it proposes will be the most cost-efficient implementation of CALEA with the least impact on subscriber rates, competition, and the introduction of new technologies. Initial comments disclose two things: first, JSTD-025 is extraordinarily expensive and second, there is an absence of cost information regarding the punch list.³

DOJ would have the Commission ignore the cost of JSTD-025 and order implementation of the entire punch list without regard to any cost information at all. DOJ believes that Section 107 actually requires the Commission to implement the punch list, no matter the cost, and apparently even if it impedes the industry's ability to develop and deploy new services that are in the public interest. This is not surprising because "CALEA AT ANY COST" has been the FBI motto from the start.

Finally, DOJ apparently no longer objects to remand to TR45.2 of any changes in the standard the Commission might order, so long as the committee is held to a

November 5, 1998).

strict schedule and the Commission retains some jurisdiction over the final product. All commenters are in substantial agreement, but process and timing are still in dispute. CTIA believes the issue should be moot because no changes in the industry standard are warranted. But if the Commission ultimately disagrees, then the Commission should permit the amendment of JSTD-025 through the normal industry process rather than the unworkable and extraordinary process proposed by DOJ.⁴

**I. SECTION 107 GIVES THE COMMISSION AUTHORITY TO
REJECT THE PUNCH LIST BASED ON THE COST OF CALEA,
AND ITS IMPACT ON SUBSCRIBER RATES AND
COMPETITION**

DOJ begins its comments by asking the Commission to put these proceedings in context. It tells the Commission that the focus of these proceeding is to "ensur[e] that law enforcement's ability to protect public safety and national security through lawful electronic surveillance is not frustrated."⁵ This is a goal that CTIA supports and one that the wireless industry meets through the many wiretaps it provisions each day. It is also a goal that industry has met through JSTD-025 -- a highly advanced standard for lawfully authorized electronic surveillance.

³ DOJ has the information regarding the aggregate cost of the punch list, but has refused to make it available to the Commission or to industry.

⁴ Industry standard setting follows strict procedural rules to accommodate anti-trust concerns. The DOJ proposal to short-circuit these procedures offends these safeguards.

But electronic surveillance is not the only goal of CALEA. Congress declared two other goals to be equally important: first, "to protect privacy in the face of increasingly powerful and personally revealing technologies;" and second, "to avoid impeding the development of new communications services and technologies."⁶ Section 107 embodies all three congressional policies on its face.

Section 107(b) is worth quoting in full and reading again because the Commission must not be misled on this critical point:

Commission Authority.--If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that

(1) meet the assistance capability requirements of section 103 by cost-effective methods;

(2) protect the privacy and security of communications not authorized to be intercepted;

(3) minimize the cost of such compliance on residential ratepayers;

(4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and

⁵ Department of Justice Comments Regarding Further Notice of Proposed Rulemaking ("DOJ Comments") at 7.

⁶ H.R. Rep. No. 103-827, 103d Cong., 2d Sess. (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3493 [hereinafter "House Report"].

(5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

Any final rule announced by the Commission must meet all five factors. The Commission may not trade one factor off against another; it cannot look a little the other way on privacy to give a little more on investigative capabilities. Nor can it ignore a little more cost to industry to enhance a few more surveillance capabilities for law enforcement. On each punch list item, the Commission must make findings on each Section 107(b) factor, each of which must be supported by evidence in the record.

A. The "Whether" and "How" of Section 107

DOJ devotes the first third of its comments arguing that the Commission's task is not to determine *whether* but *how* to implement the punch list.⁷ This, DOJ says, is required by Section 107, warning that "[w]hat the Commission may not do . . . is to adopt technical standards that stop short of 'meeting the assistance capability requirements of section 103.'"⁸

The Commission should read carefully because DOJ selectively quotes Section 107(b)(1). DOJ deletes the critical limiting language of the provision, which does

⁷ DOJ Comments at 11.

⁸ DOJ Comments at 12.

provide that the Commission must "meet the assistance capability requirements of section 103," but "by cost-effective methods."

The selective reference underscores the falseness of the "CALEA AT ANY COST" approach. To be clear, under Section 107(b)(1), if a capability cannot be provided by a cost-effective method, the Commission cannot require it at all.

Congress empowered the Commission to make this very determination, stating:

if a service of [sic] technology cannot reasonably be brought into compliance with the interception requirements, then the service or technology can be deployed. This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped.⁹

Thus, if a service or technology cannot reasonably be brought into compliance with CALEA's surveillance requirements, the service or technology can be deployed in any case.¹⁰ If the Commission has the greater power to permit the deployment of technology that cannot be wiretapped at all, it necessarily has the lesser power to permit deployment of technology with fewer enhanced surveillance features.

Another way to illustrate the point is to ask what tradeoff DOJ would have the Commission make between privacy, competition, rates or introduction of innovative,

⁹ House Report at 3499.

¹⁰ House Report at 3507.

new services and cost-efficient implementation. But first recall the instructions of Congress to the Commission:

In taking any action under this section, the FCC is directed to protect privacy and security of communications that are not the targets of court-ordered electronic surveillance and to serve the policy of the United States to encourage the provision of new technologies and services to the public.¹¹

There can be little doubt, for example, that permitting a carrier to deliver the entire packet of a packet-mode communication to law enforcement on a pen register order would be cheaper than devising means to remove and deliver addressing information alone. Yet, the Commission has tentatively concluded, on the legal grounds that content may not be delivered to law enforcement on less than a Title III order, that such a procedure is not acceptable.¹² CTIA submits that the Commission should reach the same conclusion on Section 107(b)(2) privacy grounds.¹³

How much are subscribers to pay for surveillance features? How long are they to wait for new services that enhance the public interest and further the policy of the

¹¹ House Report at 3507 (emphasis added).

¹² FNPRM, ¶ 63.

¹³ CTIA notes that full packet delivery may be cheaper, but it doesn't protect privacy. The record does not disclose whether stripping addressing information from the packets in transit is cost-efficient.

United States to promote technology?¹⁴ Of course, the FBI already has answered that preventing the introduction of new services certainly is an acceptable tradeoff to them.¹⁵ But, as noted above, that notion was rejected by Congress in 1994.¹⁶ It is ironic that it forms the basis of DOJ's arguments to the Commission in these proceedings.

It is all the more ironic because DOJ's current logic leads to the unsupportable result that the Commission can publish a final rule that no carrier can implement due to cost. The DOJ solution? Let the carriers and the Commission deal with the

¹⁴ It was recently reported by the Yankee Group that new segments of wireless users are emerging, specifically, those with annual income levels below \$20,000. This segment has doubled over the past year and the Yankee Group reports that it is the result of decreasing wireless pricing. *See Looking for the Next Generation of Wireless Users* (December 9, 1998). The price elasticity for this user segment obviously is quite low so the introduction of expensive surveillance features will have the greatest impact on those that can least afford wireless services.

¹⁵ *See Implementation of Section 109 of the Communications Assistance for Law Enforcement Act: Proposed Definition of "Significant Upgrade or Major Modification"*, 63 Fed. Reg. 23231, 23234 (April 28, 1998). There the FBI stated:

Carriers do not modify or upgrade equipment at random; such business decisions are made so that they will ultimately increase a carrier's revenue. With the promulgation of this definition, [proposed significant upgrade rule] carriers will be able to factor the requirements and costs of CALEA compliance into their decisions, thereby being able to determine if upgrading or modification is the best decision at that time.

Thus, in the FBI's view, if a carrier cannot afford to buy the entire CALEA compliance package, it cannot make the new services available at all.

¹⁶ House Report at 3499.

consequences later on an individual carrier basis through Section 109 reasonable achievability petitions.¹⁷ No one, including DOJ, will benefit from the years of protracted litigation that will be required to allocate the cost of the otherwise unaffordable CALEA solution.

In sum, the Commission's role under Section 107 is not to announce a rule that is not reasonably achievable on its face. The Commission has the power to reject outright any feature or attribute of JSTD-025 or the punch list that fails to satisfy the Section 107(b) factors. Notwithstanding, against this backdrop, it is necessary to respond to several other erroneous DOJ arguments under Section 107.

B. Punch List Alternatives

DOJ's "How, not Whether" argument has another dimension that also must be rejected. The consequence of DOJ arguing that cost information is only relevant "in choosing among the alternatives" to meet compliance is that there must be some alternative to consider.¹⁸

The Commission, to satisfy DOJ's view of the law, would have had to focus the FNPRM on the comparative costs of implementing the punch list as proposed by DOJ

¹⁷ DOJ Comments at 10. Industry comments show that the cost of compliance with just the core features of JSTD-025 will exceed \$4 billion. Even without the addition of a single punch list item, the Commission likely will see Section 109 petitions for relief.

¹⁸ DOJ Comments at 12.

and meeting the assistance capability requirements some other way. This is an odd argument from DOJ inasmuch as it argued in its deficiency petition that its proposed rule was the only possible way to implement the punch list.¹⁹

Notwithstanding, the Commission has not asked for alternative means of implementing the punch list. No party has proposed cheaper or more efficient means of doing so. That was not the scope of the FNPRM. Thus, there is no record upon which the Commission can base any conclusion regarding whether the Section 107(b) factors are met for the punch list under DOJ's interpretation.²⁰

C. DOJ's Incremental Cost Argument

DOJ next argues that the cost of complying with JSTD-025 is not relevant at all. The reason?

Carriers who choose to rely on the safe harbor created by the J-Standard must bear the costs associated with modifying post-1/1/95 equipment, facilities, and services to comply with the J-Standard, regardless of the outcome of this proceeding. The costs

¹⁹ Department of Justice and the Federal Bureau of Investigation Joint Petition for Expedited Rulemaking, filed March 27, 1998, at 25. Even if DOJ was correct, in response to the DOJ argument in opposition to a blanket industry extension under Section 107(c), the Commission recognized the need for administrative efficiency and to avoid undue burden on industry to handle similarly situated carriers in an omnibus proceeding. *See Petition for the Extension of the Compliance Date under Section 107 of the Communications Assistance for Law Enforcement Act by AT&T Wireless Services, Inc., Lucent Technologies Inc., and Ericsson Inc.*, Memorandum and Order, FCC 98-223, released September 11, 1998.

²⁰ The record does contain a detailed technological review of DOJ's proposed rule and all of its deficiencies. *See* CTIA Comments, Appendix A, dated May 20, 1998.

of implementing the J-Standard are, for present purposes, "fixed costs."²¹

But the scope of the Commission's cost-efficiency inquiry is defined by Section 107 itself. It states that "the Commission [must] establish, by rule, technical requirements or standards" that satisfy the Section 107(b) factors. It is the Commission's final rule, not just the punch list features DOJ desires to add to it, that must be cost-efficient, must protect privacy, must promote innovation and competition and must minimize the impact on subscriber rates.²²

It is not surprising that DOJ would like the Commission to overlook the cost of JSTD-025. Based on the initial comments in this proceeding and the information submitted by carriers regarding the costs of implementing JSTD-025, compliance will cost these carriers in excess of \$4 billion for the core elements of JSTD-025 alone. It will be an order of magnitude higher for all industry.²³

²¹ DOJ Comments at 17.

²² In any event, the Commission certainly could conclude on the record before it that the industry standard alone is the most cost-efficient implementation alternative to adding punch list items. This is not to say that the standard is reasonably achievable under Section 109 for all carriers. Any carrier, based on a host of factors including the cost of implementation and the effect on subscriber rates and competition, may seek relief from the Commission under Section 109 based on its own individual circumstances.

²³ CTIA has been conducting its own survey of wireless carrier costs through an independent, third party accounting firm. The preliminary survey results indicate that average upgrade costs per switch for wireless carriers will be \$756,091 for the JSTD-025 alone. (The survey defined "Upgrade Costs" as (1) vendor charge for Hardware (capability), (2) vendor charge for Software (capability), (3) Capacity Hardware, and (4) the Delivery

What is surprising is that the only party to these proceedings that has information concerning the aggregate cost of the punch list has refused to provide it. As noted in the CTIA Comments, the Attorney General requested such information in Spring 1998 and industry provided her with cost information on an expedited basis.²⁴

The Attorney General has not released the information to industry or the public, as she promised, and she has not answered the joint request of the major industry associations to make the information available to the Commission and to disclose her methodology and assumptions in reaching her conclusions.²⁵

Similarly, DOJ refused to provide cost information²⁶ to the Commission in its comments, claiming the information in its possession is covered by nondisclosure agreements. As CTIA noted in its initial comments, the FBI had sought and obtained

Function, if not vendor provided.) Average operational costs per switch per year to comply with the CALEA requirements, including direct costs and indirect costs, are expected to be approximately \$118,168. Although the data is less complete, an additional \$299,458 in upgrade cost per switch is expected for the punch list. As further data is gathered and analyzed, CTIA may seek to supplement the record.

²⁴ CTIA Comments at 6-7.

²⁵ See CTIA Comments, Exhibit A (citing Joint Industry Association letter dated December 4, 1998).

²⁶ DOJ laments that it only obtained *price* information from certain manufacturers instead of *costs*. DOJ Comments at 16. The significance of this distinction is lost on CTIA because Section 106 of CALEA clearly and unambiguously requires manufacturers to make available CALEA compliant equipment in a timely manner and at a "reasonable charge." 47 U.S.C. § 1005(b). The manufacturer's cost of producing the equipment is no more relevant to

permission to disclose data to Congress and that the agreements permitted disclosure in the aggregate.²⁷ But, inexplicably, DOJ has not sought permission to disclose the aggregated information as part of its submission to the Commission.

Thus, based on the record before it, the Commission cannot reach any conclusion about whether any punch list item can be implemented in a cost-efficient manner. But it can determine based on the record before it that no more than JSTD-025 is cost-efficient. That is, JSTD-025 -- costing more than \$4 billion -- is as far as industry can go and still meet Section 103's requirements.

D. Gold-Plating the Standard

Perhaps realizing the weakness of its substantive legal arguments in favor of the punch list, DOJ floats the idea that the Commission actually can *add* non-CALEA features to the standard because, after all, the standard is only voluntary.²⁸ Indeed, DOJ says the Commission need not worry at all about acceptance or adoption of these additional features across the industry, what DOJ terms seeking "the lowest common denominator."²⁹ According to DOJ, the Commission can develop standards and

the FBI than it is to the carrier, which must pay the invoice amount or price charged by its vendor.

²⁷ CTIA Comments at 6-7.

²⁸ DOJ Comment at 8.

²⁹ DOJ Comments at 8.

presumably adopt the punch list "without having to attempt to tailor those standards to the peculiar circumstances of individual carriers and platforms."³⁰

First, DOJ does not bother to explain how gold-plating the final standard could ever be cost-efficient and therefore meet Section 107. Nor does DOJ identify the source of the Commission's authority to require features or capabilities not in CALEA itself. Of course, the answer is that no such requirements can be imposed.

Second, DOJ seems to have forgotten its CALEA charge "to ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103" through industry standard setting.³¹ Section 107 provides no avenue for the Commission to add gold-plated features to the standard that fail to meet the Section 107(b) factors or are otherwise not required by CALEA itself.

E. Carrier Data

Having withheld its own aggregate cost information on the punch list, DOJ next cautions the Commission not to rely on data submitted by carriers.³² Indeed, DOJ wrongly states that carriers have the "obvious incentive to maximize the claimed

³⁰ DOJ Comments at 8.

³¹ 47 U.S.C. § 1006(a) (emphasis added).

³² DOJ Comments at 17.

costs of implementing CALEA . . . and to minimize [its] professed ability to meet those requirements in a cost-effective manner."³³

Carriers obtain their price information from their vendors; they do not make it up. There is no reason to believe that manufacturers have intentionally inflated or overstated the prices quoted for implementation of JSTD-025 or the punch list or that carriers themselves have done so before the Commission.³⁴ In fact, the cost data submitted in comments is remarkably consistent across platforms and manufacturers.

Further, DOJ has the manufacturer cost data and certainly could compare carrier submissions in these proceedings with that vendor information. But the answer to DOJ's caution is to put the information DOJ possesses on the public record. Section 107(b) proceedings are "intended to add openness and accountability to the process of finding solutions to intercept problems."³⁵

Finally, the suggestion that any carrier would intentionally mislead the Commission in these proceedings is beneath dignifying. Carriers have proceeded in good faith and have worked to provide the information the Commission seeks.

³³ DOJ Comments at 17.

³⁴ Nor is there any reason to assume that the manufacturers have provided DOJ with one set of prices and carriers with another.

³⁵ House Report at 3507.

II. JSTD-025 AMENDMENT

CTIA supported the Commission's decision to remand any changes in the standard to TIA's Subcommittee TR45.2 as the most efficient way to implement the Commission's final order.³⁶ DOJ accepts this conclusion, but not without a price.

A. DOJ's Unlawful Delegation Claim

DOJ maintains that the Commission's decision to remand any changes in the standard to TR45.2 is an improper delegation of its authority.³⁷ Indeed, with fair warning, DOJ says that the delegation "might expose the Commission's action to a legal challenge."³⁸

The basis of DOJ's claim is that Section 107 requires the Commission itself to establish the technical requirements or standards by rule.³⁹ CTIA, in fact, agrees that the Commission must promulgate a rule. But CTIA, like others, has urged the Commission to set the rule in broad principles so that industry could bring its genius to bear in setting standards to implement the requirements.⁴⁰

³⁶ FNPRM, ¶ 133.

³⁷ DOJ Comments at 31.

³⁸ DOJ Comments at 31. DOJ, of course, is the only party to have objected to the remand so the source of the legal action is clear.

³⁹ DOJ Comments at 31.

⁴⁰ *See, e.g.*, AT&T FNPRM Comments at 23-24.

DOJ apparently does not understand that technical requirements may be cast as general principles so that a standards organization can develop more detailed specifications.⁴¹ Yet, this is exactly the path followed by Congress when it delegated the task to industry to develop detailed standards to implement the Section 103 assistance capability requirements in the first instance.⁴²

As Congress noted, "[t]he authority to issue standards to implement legislation delegated here to private parties is well within what has been upheld in numerous precedents."⁴³ The delineation of the four Section 103 assistance requirements was considered by Congress to provide "much greater specificity than found in many delegations upheld by the courts."⁴⁴ Thus, the Commission should not hesitate to establish the broad principles and leave implementation to the industry experts.

B. DOJ's Proposal for a Rulemaking in Lieu of Ballot Resolution

DOJ proposes that the revised standard "be presented to the Commission, immediately upon its adoption, for review and (if necessary) modification by the

⁴¹ DOJ Comments at 32.

⁴² House Report at 3506-07.

⁴³ House Report at 3507.

⁴⁴ House Report at 3506-07 (citations omitted).

Commission itself."⁴⁵ In essence, DOJ seeks to preempt the standards process and substitute a rulemaking procedure after the Commission already has announced the technical requirements that industry is to implement by rule. This procedure makes no sense and certainly will lead to further delay.

Further, DOJ knows the standards process well. A proposed standard is "adopted" only after balloting and validation by TIA that the procedures to achieve consensus were followed.⁴⁶ The comment process on a proposed industry standard is open to all interested parties. No one is excluded and all comments are considered and resolved. In many respects, it is the technical equivalent of public comment under administrative law.

Apparently, DOJ is proposing that the Commission act as a super-standards plenary with a 30-day public comment period in lieu of the standards comment period and another 60 days for the Commission to resolve any disputes. CTIA fails to see how the Commission will be better suited than the standards body itself to resolve technical comment.

⁴⁵ DOJ Comments at 31.

⁴⁶ See TIA Comments at 10-14. DOJ Comments at 33 ("Before the industry standard-setting process is complete, revision to the J-Standard will be submitted for balloting.")

In the standards setting body, ballot comments are subjected to the same consensus requirements as a contribution during the development phase. The technical merit of a comment is debated and consensus achieved on its resolution. A formal notice and comment procedure before the Commission as advocated by DOJ has no similar means to resolve comments. It is more likely that any Commission technical decision made under that procedure would be challenged as arbitrary.

But the interesting part of DOJ's proposal, however, no doubt was not intended. DOJ's procedure would take at least 90 days after the "adoption" of the standard to complete. Thus, DOJ concedes that review and resolution of comment on any recommended changes to the standard is necessary and will occur after the proposed 180-day amendment cycle under either the DOJ or industry process.⁴⁷

C. DOJ's Call for Strict Compliance with the 180-day Amendment Cycle

DOJ insists that the Commission make clear that it will require "strict compliance" with the proposed 180-day time limit for amendment of the standard. If TR45.2 fails to submit the required revisions by the deadline, DOJ asks the

⁴⁷ CTIA would support a notice in the Federal Register informing the public that any amended standard is available for comment and the TIA procedures to do so.

Commission to simply adopt law enforcement's proposed rule as the penalty. Under no circumstances, DOJ says, should the Commission extend the period.⁴⁸

CTIA noted in its comments that the 180-day cycle likely would be insufficient.⁴⁹ CTIA noted, and TIA concurred in its comments, that many of the engineers that have responsibility for electronic surveillance on the TR45.2 subcommittee also are committed to other industry and TIA standards efforts, which include Y2K compliance and such important Commission mandates as number portability and E911.⁵⁰ Further, it is axiomatic that the more capabilities required by the Commission, the more complex the development and the more time that will be required to complete the task. Therefore, it is putting the cart before the horse to specify a deadline before the Commission defines the tasks.

The Commission is obligated under Section 107(b)(5) to impose only reasonable conditions in the transition to any new standard. Any schedule that would require significant disruption of established standard-setting procedures or cause slippage in established schedules for meeting other regulatory mandates inherently would be unreasonable.

⁴⁸ DOJ Comments at 33.

⁴⁹ CTIA Comments at 35. CTIA proposed as an alternative to a date certain, that the Commission should task the subcommittee to report a schedule after its first meeting, which the Commission could alter if it disagreed.

D. Delay in Revising the Standard

DOJ argues that strict conditions on the remand are necessary because "relying on TR45.2 assistance in the standard-setting process creates a risk of delay that could prejudice the timely implementation of CALEA's assistance capability requirements."⁵¹ CTIA rejects the repeated DOJ suggestions in its comments that industry standards setting efforts somehow have proceeded in bad faith or would in the future.

The very fact that only five of the FBI's 11 original punch list items were even tentatively accepted by the Commission, and that DOJ itself rejected 2 of the punch list requirements, is absolute proof of industry's good faith and judicious caution.

Notwithstanding the best of intentions, however, no one can predict whether the standards process will suffer delay anymore than the Commission could guarantee that it would or could publish a revised standard, incorporating or resolving all comments, within 180 days or some other arbitrary period. Nonetheless, industry is committed to implementing any changes ordered by the Commission with diligence.⁵²

⁵⁰ TIA Comments at 12, n. 29.

⁵¹ DOJ Comments at 32. DOJ also claims that conditions are needed "to ensure that industry's standard-setting efforts lead to a satisfactory outcome" and because "the balloting process itself could be stretched out almost indefinitely." *Id.* at 33.

⁵² To keep the Commission informed of progress, CTIA would support providing monthly meeting reports to the Commission. DOJ also has echoed the industry proposal that

E. The Role of the Enhanced Surveillance Standard ("ESS")

The Commission is well aware that industry has been attempting to standardize the punch list in consultation with the FBI through another standard's setting effort known as the ESS process. As CTIA noted in its comments, the process has been frustrating because the FBI would never overtly agree to any modification of its proposed rule. Whenever industry identified a technical weakness or better means of providing a solution, the FBI refused to accept the proposal. Thus, it is a little self-serving for DOJ to invoke the ESS process as a reason to support a strict 180-day amendment cycle.⁵³

Since the initial comments were filed, CTIA wrote the FBI to express its concern regarding the future of the ESS.⁵⁴ Months earlier, CTIA had asked the law enforcement ESS representatives to state whether the ESS text was satisfactory.⁵⁵ Rather than provide any detailed contribution reflecting proposed changes, law enforcement simply provided a comparison of the ESS document with law enforcement's proposed rule pending before the Commission.

the Commission consider assigning a technical observer to attend and report on the standards process. DOJ Comments at 33. CTIA also supports the idea.

⁵³ DOJ Comments at 32.

⁵⁴ See Letter to CALEA Implementation Section (Dec. 29, 1998), attached as Exhibit A.

Further, despite repeated requests by industry participants, law enforcement ESS representatives refused to confirm that any capabilities ruled outside of the scope of CALEA by the Commission remained of interest to, and would be purchased by, law enforcement. The FBI again refused to confirm that it would acquire these features.

CTIA requested that law enforcement specifically confirm at the January 11, 1999 ESS meeting whether or not law enforcement intended to acquire any capabilities not included in the standard by the Commission. CTIA noted that to continue the ESS process would be futile if law enforcement had no interest in purchasing the final product and it would be a serious distraction for industry engineers that already are pressed for resources to meet the deadlines imposed by the Commission for JSTD-025.

Just prior to the meeting, the FBI responded that the current ESS document "clearly" does not meet law enforcement requirements. The FBI pointed to its "comparison" contribution to explain the deficiencies, which were that any technical requirement that was not identical to the FBI's proposed rule. Further, the FBI stated

⁵⁵ The ESS document, of course, reflects the law enforcement customer perspective with none of the optimization that the industry would provide if the requirements were more clear.

that it could not judge the ESS until the Commission ruled in this proceeding.⁵⁶ Given the FBI stance on the ESS, the ESS subcommittee has suspended further work.

The Commission therefore should understand that the ESS will not yield substantial time savings in designing the final standard and should not base the schedule in reliance on ESS work to date. The ESS process was not designed to optimize the surveillance capability from a carrier-vendor perspective, but rather to identify the law enforcement "customer" requirements and preferences.

F. The Need for Specificity in the Final Order

In light of the ESS experience, CTIA believes that specificity is required in the Commission's final order. DOJ agrees. But to DOJ, that simply means adopting its proposed rule without change.⁵⁷

Instead, the Commission should adopt broad statements of principle to define any new requirements it finds. For example, rather than require industry to provide a party hold, join or drop message, the Commission should require that carriers report dynamic changes in parties to a multi-party call. In that way, the standards-setting

⁵⁶ The CIS response to CTIA is attached at Appendix B.

⁵⁷ DOJ Comments at 34 ("we encourage the Commission to refer to Appendix 1 of the Government Petition for a precise description of the capabilities that should be added to correct those deficiencies.").

body can develop the most practical means of implementing the requirement. This approach is consistent with the intent of Congress:

The legislation provides that the tele-communications industry itself shall decide how to implement law enforcement's requirements. . . . This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and finding ways to meet them without impeding the deployment of new services.⁵⁸

G. Compliance Date

There at least appears to be substantial agreement that any changes required by the Commission will take at least 18 months after new standards are promulgated to achieve.⁵⁹ Thus, DOJ urges that, pursuant to Section 107(b)(5), the deadline for compliance with the new standard should be 24 months after the final order of the Commission.⁶⁰

But the Commission must ensure that carriers have sufficient time to implement the changes across the network. The Commission should be flexible in its final order, and it should consider bundling the CALEA upgrade with other normal

⁵⁸ House Report at 3499.

⁵⁹ DOJ Comments at 29.

⁶⁰ DOJ's math does not add up. It arrives at the 24-month time period by combining the 180-day amendment cycle with the 18 month development period. Somewhere in its calculation, DOJ lost the 90-days for review and approval of the amended standard, whether by industry or the Commission. DOJ Comments at 29-30.

upgrades that will occur in the months following commercial availability of the product.

III. REASONABLY AVAILABLE CALL-IDENTIFYING INFORMATION

The Commission asked for comment under each punch list item regarding whether the information sought is "reasonably available."⁶¹ As CTIA noted in its comments, industry already addressed this issue in JSTD-025, defining reasonably available call-identifying information as "information is present at an Intercept Access Point (IAP) for call processing purposes."⁶²

DOJ, however, now points to the JSTD-025 definition as a "deficiency" that the Commission must correct.⁶³ DOJ has two basic complaints. First, the industry definition requires the information to be present at an IAP and does not require modification of existing network protocols to make it so. Second, the industry definition requires the information be present for call processing purposes.

⁶¹ FNPRM, ¶ 25-26.

⁶² JSTD-025, ¶ 4.2.1.

⁶³ DOJ Comments at 19-20.

On the first point, DOJ objects because JSTD-025 does not specify where IAPs will be located.⁶⁴ This is a specious argument because the IAPs in JSTD-025 are designed to intercept call-identifying information and call content. The suggestion that a carrier "may select IAPs that seriously limit, or even prevent altogether, the collection of call-identifying information" is factually wrong under the standard itself.⁶⁵

For example, JSTD-025 provides that the call-identifying information IAP will "provide[] expeditious access" to call-identifying information and "may span several functional entities."⁶⁶ JSTD-025 also identifies a circuit IAP to "access the call content of circuit-mode communications to or from the equipment, facilities or services of an intercept subject."⁶⁷ There is a similar requirement for the Packet Data IAP.⁶⁸

Thus, the allegation that IAPs can be established by a carrier to avoid these functions is without any foundation. Indeed, a carrier that attempted to implement the standard in a way to avoid access to call-identifying information or call content would

⁶⁴ DOJ Comments at 21.

⁶⁵ DOJ Comments at 22.

⁶⁶ JSTD-025, ¶ 4.4.

⁶⁷ JSTD-025, ¶ 4.5.1.

not be "in compliance with publicly available technical requirements" so as to have a safe harbor.⁶⁹

The second part of DOJ's concern is that network protocols need not be modified to make call-identifying information reasonably available. The concern is based on the false DOJ premise that systems must be redesigned to create new information for law enforcement's use.⁷⁰ As Congress said, "if such information is not reasonably available, the carrier does not have to modify its system to make it available."⁷¹

Indeed, CTIA questioned in its comments whether the Commission itself meant to imply in the FNPRM that if call-identifying information *could be reasonably made available* in the future, a carrier would have to redesign network protocols today to provide it.⁷² Such a conclusion would be wrong because the legal standard under

⁶⁸ JSTD-024, ¶ 4.5.2.

⁶⁹ 47 U.S.C. § 1006(a)(2).

⁷⁰ DOJ notes that the Commission has required modification of network protocols in other proceedings. While that may be true, none of the situations referenced by DOJ were statutory in nature or accompanied by an express limitation that the information be "reasonable available" to the carrier.

⁷¹ House Report at 3501.

⁷² For example, in regard to customer premises equipment (CPE), the Commission concluded that "party hold/join/drop information *could not be reasonably made available to the LEA* since no network signal would be generated." FNPRM, ¶ 86 (emphasis added).

CALEA is whether call-identifying information *is* reasonably available, not whether it could be made so in the future.⁷³

The second DOJ objection relates to the JSTD-025 requirement that call-identifying information be present at the IAP for call processing purposes. But the standard's definition is consistent with that used by Congress to define call-identifying information in the first place as dialing or signaling information used for "the purpose of routing calls through the telecommunications carrier's network."⁷⁴

DOJ contends that the JSTD-025 definition would permit carriers to withhold call-identifying information. This argument is based on the parties' different definitions of call-identifying information. If the Commission accepts the DOJ position in these proceedings and adds certain punch list items to the standard, then DOJ may be correct. But, if the Commission follows the direction of Congress in limiting call-identifying to that information that routes a call through a carrier's network, then no change at all would be required.⁷⁵

⁷³ What is more, Congress clearly and unequivocally excluded CPE and the by implication the signals it generates from CALEA. House Report at 3503.

⁷⁴ House Report at 3501.

⁷⁵ DOJ notes that the Commission has tentatively concluded that post-cut-through dialed digits are call-identifying and that the reasonable availability definition in JSTD-025 would preclude delivery of this information. The contention is completely false. The information can and should be obtained by law enforcement through the circuit IAP or from the long distance carrier at its call-identifying IAP.

Moreover, changing the definition to that proposed by DOJ would greatly expand the definition of reasonably available. Essentially, as proposed by DOJ, any signal anywhere in the network would be reasonably available. This would be the case whether or not the signal can be accessed in the particular network element where it resides so long as it can be delivered to an IAP somewhere.⁷⁶ The Commission might ask what signal would not fit this definition. For its part, CTIA can think of no signal that would not be reasonably available under the DOJ definition.

In sum, the Commission should accept the industry's definition of reasonably available without modification. Implicitly, this requires the Commission to accept the definition of call-identifying information provided by Congress rather than the expansive definition proffered by DOJ.

IV. THE PUNCH LIST

The Commission has received an overwhelming amount of legal analysis explaining why the DOJ punch list exceeds the scope of Section 103 of CALEA. The CTIA Comments as well as those of other parties can be read side-by-side with the DOJ Comments; little more is required for the Commission to reach its conclusions of law. Instead of further legal argument, CTIA will confine its comments to several new or novel ideas raised in the DOJ Comments.

⁷⁶ DOJ Comments at 25.

A. The National Wiretap Plan

In its discussion of conference call content, DOJ floats a new idea fraught with grave consequences. It suggests that wireless carriers have an obligation to continue providing call content or call-identifying information when the subscriber leaves his or her service area.⁷⁷ In essence, DOJ proposes a nation-wide wiretap obligation for wireless carriers.

But DOJ again stretches CALEA too far. Section 103 requires a carrier to expeditiously isolate and enable the government to intercept all wire and electronic communications "carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier."⁷⁸ This, the government says, is no limitation at all and urges the Commission to read it to say "carried within any service area."⁷⁹

DOJ asks the Commission to order wireless carriers to make available call content through the original IAP within the service area covered by the order or to ensure that law enforcement is able to access the conference call without loss of

⁷⁷ DOJ Comments at 40. DOJ offers this new idea in response to the Commission's valid observation that when a conference call is rerouted to another service area, the carrier's obligation ends. FNPRM, ¶ 78.

⁷⁸ 47 U.S.C. § 1002(a)(1) (emphasis added).

⁷⁹ DOJ Comments at 40.

content through another IAP.⁸⁰ The Commission should understand that this would require a wireless carrier to implement a wiretap in every switch upon receipt of an order.⁸¹ This cynical reading of Section 103 should be rejected completely.

It is also belied by the mobile assistance requirements of Section 103, which provide:

A telecommunications carrier that is a provider of commercial mobile service (as defined in section 332(d) of the Communications Act of 1934) offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of wire or electronic communication service that has acquired access to the communications.⁸²

⁸⁰ DOJ Comments at 40-41.

⁸¹ Routing the call back through the original IAP is a veiled attempt to save the government provisioning charges for the necessary lines to transport the call.

⁸² 47 U.S.C. § 1002(d) (emphasis added).

In short, when the services at issue are transferred to another service area or another carrier,⁸³ the carrier's obligation ends with notice to the government, which of course is provided for in JSTD-025.⁸⁴ This is not to say, of course, that a carrier need not be compliant with Section 103 in every service area-it must-but CALEA requires no more.

B. CALEA Is Not a Strict Liability Statute

The Commission has rejected three of DOJ's punch list items at beyond the scope of Section 103: surveillance status,⁸⁵ continuity check⁸⁶ and feature status.⁸⁷ DOJ lumps these features under the rubric "surveillance integrity" and claims the Commission fails in its duty to "ensure" carriers meet Section 103 at all times.⁸⁸ DOJ is wrong, CALEA is not a strict liability statute.

Specifically, and falsely, DOJ states that "the J-Standard excuses carriers from taking any such steps" to "ensure surveillance integrity."⁸⁹ It does no such thing. To

⁸³ DOJ concedes the point as it relates to another carrier. DOJ Comments at 41, n. 6.

⁸⁴ JSTD-025, ¶ 4.3.

⁸⁵ FNPRM, ¶ 106.

⁸⁶ FNPRM, ¶ 111.

⁸⁷ FNPRM, ¶ 116.

⁸⁸ DOJ Comments at 58.

⁸⁹ DOJ Comments at 58.

the contrary, it affirmatively requires carriers to implement surveillance whenever authorized. Whenever surveillance begins, a message must be sent; whenever it ends, a message must be sent; and whenever prescribed events occur in between, a message must be sent. CTIA fails to understand the accusation that the standard excuses compliance.

What DOJ really argues for is a strict liability standard and a super-reengineering effort to design systems that are fail-safe for surveillance even if such capabilities go beyond the norm for call processing. If the Commission accepts the DOJ position that the use of the word "ensure" in Section 103 requires "affirmative steps to ensure surveillance integrity", then in all future discussions, DOJ will argue that the Commission's decision requires extremely fine fault tolerances for equipment, priority access for subjects of surveillance, queuing and buffering of call-identifying information, redundant systems and a host of other measures to "ensure" compliance. Indeed, there is no end to DOJ's imagination when it comes to ensuring surveillance capabilities, especially when the price is no object.

Fortunately, DOJ relies too much on the use of the term "ensure" in Section 103. Congress plainly meant for "carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber

who is the subject of a court order authorizing electronic surveillance."⁹⁰ The use of the term in Section 103 has nothing whatsoever to do with surveillance integrity.⁹¹ This is underscored by the fact that Congress did not even use the word "ensure" once to describe the Section 103 requirements in the accompanying House Report.⁹²

In sum, the Commission was correct to reject the three punch list items demanded by DOJ as beyond the scope of CALEA. No further requirements, automated or regulatory, are warranted or authorized by CALEA.⁹³

C. Post-Cut-Through Digit Extraction

DOJ admits that there must be either an out-of-switch solution developed or "the originating carrier's hardware will have to be modified" to provide post-cut-through dialed digits.⁹⁴ Moreover, DOJ agrees that no solution exists today to distinguish such digits from other content, but they would welcome (but apparently not fund) the industry development of such a solution.

⁹⁰ House Report at 3590.

⁹¹ Indeed, it is Section 105 of CALEA that addresses "systems security and integrity" and the focus of that provision is unlawful surveillance by government through remote access to carrier facilities. *See* 47 U.S.C. § 1004; House Report at 3506.

⁹² House Report at 3501.

⁹³ This is not to say that DOJ is without recourse if a carrier consistently fails to comply with a surveillance order or CALEA's requirements. Its remedy is an enforcement action under Section 108.

⁹⁴ DOJ Comments at 67.

While DOJ may call post-cut-through dialed digits "call-identifying", it cannot refute the fact that the subject's carrier has completed the call when the connection is made to the long distance carrier. The dialed digits are only call-identifying to the subsequent carrier. CALEA does not require, and the Commission cannot impose on the originating carrier, an obligation to develop technology to extract the call identifying information of another carrier.⁹⁵

Of course, DOJ has full access to such information either by going to the long distance carrier directly with an appropriate order or by serving a Title III order on the originating carrier and provisioning a content channel. CTIA sees no reason why an appropriate court order could not be tailored to obtain a content channel to extract post-cut-through dialed digits. An order requiring the carrier to provide such technical assistance would be honored, and the CALEA mandate to protect the privacy of communications not authorized to be intercepted would be preserved through court-supervised minimization requirements. This is the most cost-efficient means to implement this requirement if the Commission mandates it.

⁹⁵ Further, Section 107(b)'s privacy mandate cannot be satisfied by placing a carrier between law enforcement and a content channel on a mere pen register order. DOJ admits that carriers cannot distinguish between post-cut-through dialing that initiates a call through a long distance carrier and other signaling such as bank account numbers or credit card transactions.

The proof requires no calculus. Under DOJ's rule, every carrier in the nation would have to acquire DTMF tone decoders and have them installed and ready for every one of the thousands of pen register orders levied each year. Conversely, under CTIA's proposal, law enforcement could acquire relatively few decoders, pool them, and apply them on an as-needed basis.⁹⁶ It will take enormous line charges and provisioning expenses for law enforcement to make up for the cost to carriers of implementing the DOJ proposal. CTIA's approach, assuming the Commission mandates this capability, which it should not, is the more cost-efficient on its face.

In any event, CTIA still believes that this punch list item cannot meet Section 107(b)'s privacy requirement, no matter how cheaply it can be provided.⁹⁷ The Commission cannot trade privacy off against expense or government convenience in this proceeding.

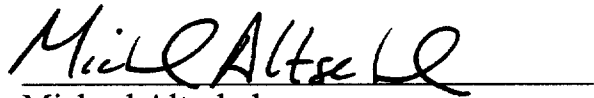
⁹⁶ Further, as CTIA noted in its comments, for wireless carriers, DTMF tone decoders are unnecessary. The numbers dialed are sent over the air interface after the subscriber hits the SEND key unlike in wireline systems where tone decoders circuits are used to gather digits as they are pulsed from a landline phone. Thus, major software changes would be required for most wireless switches and significant changes would be required in the engineering and capacity guidelines for mobile switching centers to accommodate the additional hardware required for each surveillance. DOJ's proposal simply is not cost-efficient for the wireless carrier.

⁹⁷ CTIA questioned in its comments whether carriers would be authorized in any case to intercept call content in order to provide extracted digits to law enforcement and asked how this would protect the privacy of the call content not otherwise authorized to be intercepted.

V. CONCLUSION

On substantive legal grounds, the Commission should reject the punch list. If the Commission still concludes some punch list items are required, the Commission must demonstrate on the record through careful analysis that the final rule will satisfy each of the Section 107(b) factors. Finally, the Commission should remand any amendments in the standard to TR45.2 and permit a reasonable term to develop the requirements.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Michael Altschul", written over a horizontal line.

Michael Altschul
Vice President and General Counsel

Randall S. Coleman
Vice President
Regulatory Policy & Law

**Cellular Telecommunications Industry
Association**

1250 Connecticut Ave., N.W.
Suite 800
Washington, D.C. 20036
(202) 785-0081

January 27, 1999

Attachment A

PERKINS COIE LLP

1201 THIRD AVENUE, 40TH FLOOR - SEATTLE, WASHINGTON 98101-3099
TELEPHONE: 206 583-8888 - FACSIMILE: 206 583-8500

ALBERT GIDARI
(206) 583-8688
gidari@perkinscoie.com

December 29, 1998

BY FACSIMILE AND MAIL

H. Michael Warren
Section Chief, CIS
Federal Bureau of Investigation
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 22021

Re: Enhanced Surveillance Standard Efforts

Dear Mr. Warren:

As you know, the Cellular Telecommunications Industry Association (CTIA) initially proposed the Enhanced Surveillance Standard or "ESS" project to provide a means to make available to law enforcement for purchase those surveillance capabilities that industry did not believe were mandated by the Communications Assistance for Law Enforcement Act (CALEA) but nonetheless were desired by law enforcement. For almost a year, industry has worked with law enforcement to understand and define its requirements in the ESS process.

Months ago, CTIA expressly asked the law enforcement ESS representatives to state whether the Stage 1 and Stage 2 ESS text was satisfactory. The ESS document, of course, reflects the law enforcement customer perspective with none of the optimization that the industry would provide if the requirements were more clear. Rather than provide any detailed contribution reflecting proposed changes, law enforcement simply provided a comparison of the ESS document with law enforcement's proposed rule pending before the Federal Communications Commission (FCC), leading some in industry to question whether the FBI was serious about working with industry to craft standardized punch list requirements.

[00000-0000/SI.983620.257]

December 29, 1998

Page 2

Further, despite repeated requests by industry participants over the last few months, law enforcement ESS representatives have refused to confirm that any capabilities ruled outside of the scope of CALEA by the FCC remain of interest to, and will be purchased by, law enforcement. Indeed, in the FBI's most recent comments on the FCC proposed capability rule, it states that, indeed, such capabilities cannot be acquired at all if not mandated by the FCC.

In light of these developments, CTIA requests that law enforcement specifically confirm at the next ESS meeting (scheduled by conference call for January 11, 1999) whether or not law enforcement intends to acquire any capabilities not included in the standard by the FCC. Obviously, to continue the ESS process would be futile if law enforcement has no interest in purchasing the final product and it would be a serious distraction for industry engineers that already are pressed for resources to meet the deadlines imposed by the FCC for the core elements of JSTD-025.

Absent law enforcement express support, the ESS project would appear to have no purpose and therefore should be terminated. Of course, following final FCC action on the disputed capabilities, should law enforcement decide it really does need these capabilities, the ESS project can be reassessed.

We look forward to your reply.

Sincerely,



Albert Bidari

AG:rg

cc: Ed Hall, CTIA (for CALEA list distribution)

Attachment B



U.S. Department of Justice

Federal Bureau of Investigation

*CALEA Implementation Section
14800 Conference Center Drive, Suite 300
Chantilly, VA 20151*

January 8, 1999

By Facsimile and U. S. Mail

Mr. Albert Gidari, Esq.
Perkins Coie, L.L.P.
1201 Third Avenue, 40th Floor
Seattle, Washington 98101-3099

RECEIVED

JAN 19 1999

PERKINS COIE

Re: Efforts on the Enhanced Surveillance Services

Dear Mr. Gidari:

As the primary representative for law enforcement on issues relating to the Communications Assistance for Law Enforcement Act (CALEA), the Federal Bureau of Investigation supports the efforts of the Telecommunications Industry Association (TIA) standards setting body TR45.2, and has participated actively in the Enhanced Surveillance Services (ESS) project. Our support of the ESS activity is evidenced by our involvement in, and significant contributions to, the process. As you know, contributions from law enforcement have formed the foundation which has allowed the ESS group to proceed to the current version of its work product, represented in PN-4177, Revision 12.

However, your December 29, 1998, letter mis-characterizes the established scope of the ESS charter. Your contention that the ESS activity was undertaken in order to standardize capabilities for "law enforcement's purchase" is not supported by the "Scope and Justification" wording expressly included in the *TIA Project Request and Authorization Form* for PN-4177, dated December 1997. The document clearly defines the "Scope and Justification" of the project as "The interface and services for enhanced electronic surveillance services beyond the scope of the J-STD-025 (or J-STD-025A)." To our knowledge, there have been no contributions which have been accepted that change that scope of the ESS activity.

Further, the bylaws of the TIA standards process leave little doubt that the primary purpose of that standards setting process is technical in nature. From the outset, the CALEA Implementation Section's (CIS) participation in the ESS process was intended to provide technical assistance to the industry by providing law enforcement's perspective regarding the standardization of certain assistance capabilities missing from the interim industry standard (J-STD-025). Matters regarding payment are typically, and more appropriately, determined outside of the technical standardization process.

Mr. Albert Gidari

Page 2

Your letter also suggests that law enforcement has failed to provide the Cellular Telecommunications Industry Association (CTIA) an answer as to whether the ESS document is satisfactory in its current form. This is not the case. The ESS work on the PN-4177 document is not yet complete. Therefore, it would be premature to make any conclusion as to the sufficiency of the document's contents. However, CIS did prepare and submit a contribution which provides a comparison of the current ESS document and law enforcement's requirements. This comparison clearly shows that Stage 2 in its current form still does not address all of law enforcement's stated requirements. Given law enforcement's five-year involvement in, and contributions to, the TR45.2 and ESS processes, I am unclear how you can question law enforcement's commitment to working with industry to standardize the missing assistance capabilities.

Law enforcement has stated in submissions to the Federal Communications Commission (FCC) that it does not contest the content of the current interim industry standard (J-STD-025), but maintains that it is deficient due to the fact that it lacks certain assistance capabilities. As we are all aware, CTIA and other industry associations disagree with law enforcement's view on this matter. While the FCC has tentatively concluded that many of the missing assistance capability items are required by CALEA,¹ no final rule has been published. Therefore, it is premature to judge the effectiveness of ESS's technical standardization activities until such time that the FCC has ruled which assistance capabilities are required by section 103 of CALEA.

Once the FCC has ruled, we see no compelling reason for TR45.2 to re-open J-STD-025, on which law enforcement and industry agree, simply to incorporate the missing assistance capabilities. To do so would cause unnecessary delays, place an unnecessary burden on industry's limited engineering resources, and would serve to negate the significant work which has been accomplished over the last 12 months. We understand there may be limited resources available to address the current ESS work, while also meeting the pressing deadline for implementation of the current industry standard (J-STD-025). Therefore, we would support a TR45.2 Plenary decision to focus first on those additional items determined by the FCC to be required.

I believe that our position on these issues is clearly stated above. For this reason, I see no need to further address these issues in the next ESS meeting scheduled for January 11, 1999, via conference call.

Sincerely,



H. Michael Warren
Senior Project Manager/Chief

¹See Further Notice of Proposed Rulemaking, CC Docket No. 97-213 (published November 2, 1998).